Amendments To Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A smartcard transaction system configured with a biometric security system, said system comprising:

a smartcard configured to communicate with a reader;

a reader configured to communicate with said system;

a keystroke scan sensor configured to detect a proffered keystroke scan sample, said keystroke scan sensor configured to communicate with said system; ~~and,~~

a device configured to verify said proffered keystroke scan sample to facilitate a transaction;

a first enterprise data collection unit associated with a first enterprise, said first enterprise data collection unit configured to store update transactions and pending transactions associated with said smartcard and said first enterprise;

a second enterprise data collection unit associated with a second enterprise, said second enterprise data collection unit configured to store update transactions and pending transactions associated with said smartcard and said second enterprise;

at least one access point configured to interface with said smartcard and said first and second enterprise data collection units;

a card object database system coupled to said first and second enterprise data collection units and configured to store said smartcard information in accordance with said update transactions and said pending transactions, wherein said smartcard information includes a card object having at least one application;

an update logic system configured to route said smartcard information from said first and second enterprise data collection units to said at least one access point in order to effect synchronization of said smartcard information associated with said smartcard and said card object database system; and,

wherein said verification device activates said update logic system upon verification of said proffered keystroke scan sample.

2. (currently amended) The smartcard transaction system of claim 1, wherein said keystroke scan sensor is configured to communicate with said system via at least one of a smartcard, a reader, and a network.

Claims 3-4(cancelled).

5. (currently amended) The smartcard transaction system of claim 1, further including a database configured to store ~~at least one~~ a data packet, wherein said data packet includes at least one of: proffered and registered keystroke scan samples, proffered and registered user information, terrorist information, and criminal information.

6. (currently amended) The smartcard transaction system of claim 5 [[4]], wherein said database is contained in at least one of the smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

7. (original) The smartcard transaction system of claim 5, wherein said remote database is configured to be operated by an authorized sample receiver.

Claim 8 (cancelled).

9. (original) The smartcard transaction system of claim 1, wherein said keystroke scan sensor is configured to detect and verify keystroke scan characteristics including at least one of behavioral, temporal and physical characteristics.

10. (original) The smartcard transaction system of claim 1, wherein said keystroke scan sensor device is configured to detect false keystrokes and body heat.

Claim 11 (cancelled).

12. (original) The smartcard transaction system of claim 11, wherein said device configured to compare a keystroke scan sample is at least one of a third-party security vendor device and local CPU.

13. (original) The smartcard transaction system of claim 11, wherein a stored keystroke scan sample comprises a registered keystroke scan sample.

14. (original) The smartcard transaction system of claim 13, wherein said registered keystroke scan sample is associated with at least one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

15. (original) The smartcard transaction system of claim 14, wherein different registered keystroke scan samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

16. (original) The smartcard transaction system of claim 14, wherein a keystroke scan sample is primarily associated with first user information, wherein said first information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein a keystroke scan sample is secondarily associated with second user information, wherein said second information comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein said second user information is different than said first user information.

17. (original) The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered keystroke scan sample.

18. (original) The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered keystroke scan sample.

19. (currently amended) The smartcard transaction system of claim 1, wherein said keystroke scan sensor is configured to provide a notification upon detection of a sample.

20. (original) The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

21. (original) The smartcard transaction system of claim 1, wherein said device configured to verify is configured to facilitate the use of at least one secondary security procedure.

Claims 22-33 (cancelled).

34. (currently amended) A method for facilitating biometric security in a smartcard transaction system comprising:

detecting a proffered keystroke scan at a sensor communicating with said system to obtain a proffered keystroke scan sample;

verifying ~~the~~ said proffered keystroke scan sample; ~~and~~

authorizing a transaction to proceed upon verification of ~~the~~ said proffered keystroke scan sample;

storing, by a first enterprise data collection unit, update transactions and pending transactions associated with said smartcard and a first enterprise, wherein said first enterprise data collection unit is associated with a first enterprise;

storing, by a second enterprise data collection unit, update transactions and pending transactions associated with said smartcard and a second enterprise, wherein said second enterprise data collection unit is associated with a second enterprise;

interfacing with said smartcard and said first and second enterprise data collection units, at an access point;

storing, by a card object database system coupled to said first and second enterprise data collection units, said smartcard information in accordance with said update transactions and said pending transactions, wherein said smartcard information includes a card object having an application;

routing, by an update logic system, said smartcard information from said first and second enterprise data collection units to said access point in order to effect synchronization of said smartcard information associated with said smartcard and said card object database system; and,

activating, by said verification device, said update logic system upon verification of said proffered keystroke scan sample.

35. (original) The method of claim 34, wherein said step of detecting further includes detecting a proffered keystroke scan at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.

36. (original) The method of claim 34, wherein said step of detecting a proffered keystroke scan includes detecting a proffered keystroke scan at least one of an electronic sensor, an optical sensor and a keyboard.

37. (original) The method of claim 34, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered keystroke scan sample.

Claims 38-40 (cancelled).

41. (original) The method of claim 34, wherein said step of detecting further includes using said keystroke scan sensor to detect at least one of false keystrokes and body heat.

42. (original) The method of claim 34, wherein said step of verifying includes comparing a proffered keystroke scan sample with a stored keystroke scan sample.

43. (original) The method of claim 42, wherein said step of comparing a proffered keystroke scan sample with a stored keystroke scan sample comprises storing, processing and comparing at least one of behavioral, temporal and physical characteristics.

44. (original) The method of claim 42, wherein comparing a proffered keystroke scan sample with a stored keystroke scan sample includes comparing a proffered keystroke scan sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

45. (original) The method of claim 34, wherein said step of verifying includes verifying a proffered keystroke scan sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

46. (original) The method of claim 34, wherein said step of verifying includes verifying a proffered keystroke scan sample using at least one of a local CPU and a third-party security vendor.

47. (New) The smartcard transaction system of claim 1, further comprising an update logic system coupled to at least one enterprise data synchronization interface, said update logic system configured to securely route card information between said enterprise data synchronization interface and said enterprise data collection units, said enterprise data synchronization interface coupled to an enterprise network configured to communicate with said access point.

48. (New) The smartcard transaction system of claim 47, further comprising a secure support client server configured to communicate with said access point, said secure support

client server further configured to adaptively provide communication functionality in accordance with the communication functionality available at said access point.

49. (New) The smartcard transaction system of claim 48, further including a personalization system comprising:

a security server;

at least one key system associated with said at least one application, said key system configured to communicate with said security server and to supply a key in response to a request from said security server;

a personalization utility configured to receive said card object and to communicate with said security server;

said personalization utility further configured to add said key to said card object, a card management system, said card management system configured to accept a card request and communicate said card request to said personalization utility; and

a gather application module configured to communicate with said card management system and gather application information from a first database and a second database in accordance with said card request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.

50. (New) The method of claim 34, further comprising securely routing, by an update logic system, card information between said enterprise data synchronization interface and said enterprise data collection units, wherein said update logic system is coupled to an enterprise data synchronization interface, and communicating, by said enterprise network, with said access point, wherein said enterprise data synchronization interface is coupled to said enterprise network.

51. (New) The method of claim 50, further comprising, by a secure support client server, communicating with said access point, and adaptively providing communication functionality in accordance with the communication functionality available at said access point.

52. (New) The method of claim 51, further comprising:

communicating, by a key system, with a security server and supplying a key in response to a request from said security server, wherein said key system is associated with said application;

receiving, by a personalization utility, said card object and communicating with said security server;

adding, by said personalization utility, said key to said card object;

accepting, by a card management system, a card request and communicating said card request to said personalization utility; and

communicating, by a gather application module, with said card management system and gathering application information from a first database and a second database in accordance with said card request, wherein said first database is associated with said first enterprise, and said second database is associated with said second enterprise.